



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993
24956	7590	07/11/2008	EXAMINER	
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.			DAVIS, ZACHARY A	
1800 DIAGONAL ROAD			ART UNIT	PAPER NUMBER
SUITE 370			2157	
ALEXANDRIA, VA 22314				
MAIL DATE		DELIVERY MODE		
07/11/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	09/940,982	ENDO ET AL.
	Examiner Zachary A. Davis	Art Unit 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(o).

Status

1) Responsive to communication(s) filed on 28 April 2008.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-8 and 18-26 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-8 and 18-26 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 28 April 2008 has been entered.
2. By the above submission, Claims 1, 4-8, 18, and 21 have been amended. New Claims 23-26 have been added. No claims have been canceled. Claims 1-8 and 18-26 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 28 April 2008 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1-8 under 35 U.S.C. 103(a) as unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518, Applicant argues that Jaffe does not disclose the new limitation of the input data D1 not having a constant Hamming weight (page 9 of the present response). First, the Examiner notes

that there does not appear to be sufficient written description for this new limitation in the present disclosure, nor has Applicant pointed out such support, and therefore the claims are rejected under 35 U.S.C. 112, first paragraph, for failing to comply with the written description requirement as set forth below. Further, to the extent that the claim can be examined, with respect to the new limitation in particular, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The Examiner acknowledges that, as Applicant asserts, Jaffe discloses that "Operations are performed using a data representation such that the Hamming weight of all input values is constant" (see page 9 of the present response, citing Jaffe, column 4, lines 58-59). However, the Examiner submits that even though the values are operated on using a constant Hamming weight data representation, at least the logic values that are initially input before the data is converted into the constant Hamming weight representation do not necessarily have a constant Hamming weight (see Jaffe, column 2, lines 57-67, where the representation of data is transformed; note that this does not necessarily refer to a specific transformation operation, as the portion at column 4, line 55-column 5, line 30, also does not necessarily refer to a specification mapping operation in contrast to Applicant's previous assertions in prior responses; however, the data at base, which is represented using the constant Hamming weight representation, may or may not itself have a constant Hamming weight). Further, the Examiner notes that the admitted prior

art is silent as to whether the input data has a constant Hamming weight, but does explicitly admit that there is no limitation placed on some of the data in the system, namely the disturbance data (page 21, lines 1-12 of the present application).

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

4. Applicant's arguments with respect to claims 18-26 have been considered but are moot in view of the new grounds of rejection. In particular, it is noted that Applicant asserts that Jaffe does not disclose the inverse transform step using the second disturbance data, as recited in independent Claims 18 and 23 (see pages 10 and 11 of the present response). However, this argument is moot, because the admitted prior art clearly discloses using the second disturbance data to perform an inverse transform function (see page 21, lines 1-12 of the present application).

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 1 has been amended to recite the limitation "wherein said input data D1 does not have a constant Hamming weight". However, the specification appears to be entirely silent as to the Hamming weight of the input data; there does not appear to be any indication as to whether the input data either would or would not have a constant Hamming weight. Therefore, there is not proper antecedent

basis for the limitation in the specification. See below regarding the rejection for failure to comply with the written description requirement under 35 U.S.C. 112, first paragraph, for further detail.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Specifically, independent Claim 1 has been amended to recite the limitation "wherein said input data D1 does not have a constant Hamming weight". First, Applicant has not pointed out where this claim limitation is supported in the present specification, nor does there appear to be written description of the above claim limitation in the application as filed. See MPEP § 2163.04(I)(B). Further, the specification appears to be entirely silent as to the Hamming weight of the input data; there is no indication in the present specification whether the input data either would or would not have a constant Hamming weight. It is noted that the absence of a positive

recitation in the specification is not basis for an exclusion (i.e. the negative limitation, that the input data does not have constant Hamming weight). See also MPEP § 2173.05(i).

Claims 2-8 are rejected due to their dependence on rejected Claim 1.

8. Regarding the rejection of Claims 18-22 under 35 U.S.C. 112, second paragraph, as indefinite, although the amendments to the claims have overcome the previous issues of indefiniteness, the amendments have also raised new issues of indefiniteness. Therefore, the claims REMAIN rejected as set forth below.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 18-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 18 recites "the m-bit random numbers" in line 7 of the claim. There is now insufficient antecedent basis for this limitation in the claim as amended, which renders the claim indefinite.

Claims 19-22 are rejected due to their dependence on rejected Claim 18.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

12. Claims 23, 25, and 26 are rejected under 35 U.S.C. 102(a) as being anticipated by Applicant admitted prior art.

In reference to Claim 23, Applicant admits as prior art an apparatus including a processor (see prior art Figure 2, CPU 201, coprocessor 202; page 2, line 14-page 3, line 5 of the present application), a storage (Figure 2, storage device 204; page 2, lines 14-17; page 3, line 8–page 4, line 2) arranged to store programs (Figure 2, program memory 205; page 3, line 12) and data (Figure 2, data memory 206; page 3, lines 12-14), and a data bus interconnecting the processor and storage (Figure 2, bus 203; page 3, lines 5-7). Applicant further admits that the processor is arranged to transform input data into first transformed data with first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data (see page 21, lines 1-12 of the present application).

In reference to Claim 25, Applicant further admits transforming data by means of an XOR operation (or an addition or transform operation) (see pages 8 and 9 of the present application, noting Expressions 3, 4, 5, 7, 9, and 10, in particular).

In reference to Claim 26, Applicant further admits performing a rotate operation, a shift operation, or a bit permutation operation (see pages 8 and 9 of the present application, noting Expressions 2, 6, and 8 in particular).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 18 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art.

In reference to Claim 18, Applicant admits as prior art an apparatus including a processor (see prior art Figure 2, CPU 201, coprocessor 202; page 2, line 14-page 3, line 5 of the present application), a storage (Figure 2, storage device 204; page 2, lines 14-17; page 3, line 8-page 4, line 2) arranged to store programs (Figure 2, program memory 205; page 3, line 12) and data (Figure 2, data memory 206; page 3, lines 12-14), and a data bus interconnecting the processor and storage (Figure 2, bus 203; page 3, lines 5-7). Applicant further admits that the processor is arranged to transform input

data into first transformed data with first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data (see page 21, lines 1-12 of the present application). However, Applicant does not explicitly disclose that the first disturbance data of n bits is generated by concatenating a predetermined number of m-bit random numbers.

Official notice is taken that it is well known that, in order to generate long random numbers, a series of shorter random numbers can be generated and concatenated together. In particular, if one only has access to a device that can generate at most m bit long random numbers, and if one needed a longer, n bit random number, then one could simply generate a plurality of m bit random numbers and concatenate sufficient of them together until the new string was n bits long. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the generation of the n bit first disturbance data by concatenating a predetermined number of m bit random numbers, in order to realize the predictable result of the generation of a longer random number of the desired length of n bits, using available hardware and/or algorithms.

In reference to Claim 20, further Official notice is taken that it is well known to collect data in a table. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a table for the m bit random numbers in order to

realize the predictable result of easier and more organized access to any of the m bit numbers that were desired to be used.

In reference to Claim 21, Applicant further admits and transforming data by means of an XOR operation (or an addition or transform operation) (see pages 8 and 9 of the present application, noting Expressions 3, 4, 5, 7, 9, and 10, in particular).

In reference to Claim 22, Applicant further admits performing a rotate operation, a shift operation, or a bit permutation operation (see pages 8 and 9 of the present application, noting Expressions 2, 6, and 8 in particular).

15. Claims 1-8, 19, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, where the input data does not have constant Hamming weight; a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application; there is no limitation placed on the disturbance data).

However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60; however, the data that is represented by a constant Hamming weight representation does not necessarily, and does not likely, have a constant Hamming weight itself). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 2, Applicant admits that the prior art further discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8 ; see also column 8, lines 41-45, and column 5, lines 12-18).

In reference to Claim 4, Applicant admits that the prior art further discloses generating processed disturbance data by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4, and Jaffe, column 4, line 55-column 5, line 30).

In reference to Claim 5, Applicant further admits and Jaffe further discloses a disturbance data storage means, disturbance data select means, and that processing is

carried out on the disturbance data in order to generate the processed disturbance data (page 21, lines 6-8 of the present application, and prior art Figure 4; Jaffe, column 16, lines 15-32).

In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number (column 7, lines 62-64; see Figures 1 and 4; see also column 5, lines 12-18), means for inverting bits of data (column 8, lines 41-45; Figure1, step 150; Figure 4, step 450), and means for concatenating a random number with data output by the means for inverting (Figure 1, steps 110-120; Figure 4, steps 410-420).

In reference to Claim 7, Jaffe further discloses a random number generation means (column 7, lines 62-64), a Hamming weight computation means (see Figure 1; column 8, lines 25-29 and 46-65), a Hamming weight examination means (see Figure 1; column 8, lines 25-29 and 46-65), and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight).

In reference to Claim 8, Jaffe further discloses random number generation means to generate partial random numbers with uniform constant Hamming weights and bit count each equal to a fraction of a final random number (Figure 1, step 115; Figure 4, step 415); means to generate random numbers until a sum of bit counts is equal to the final bit count (column 7, lines 62-64); and means for concatenating the partial random numbers (Figure 1, steps 110-120; Figure 4, steps 410-420).

In reference to Claims 19 and 24, Applicant admits as prior art everything as described above with reference to Claims 18 and 23, respectively. However, Applicant further admits that such prior art does not explicitly disclose that the disturbance data has a constant or target Hamming weight, and in particular, the prior art does not explicitly disclose that each bit in the disturbance data has a logic value of 0 or 1 at a probability of 50%.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). More specifically, Jaffe discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8 ; see also column 8, lines 41-45, and column 5, lines 12-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, where the disturbance data has appearance probabilities of 50% for either 0 or 1 for each bit, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. M'Raihi et al, Publication FR 2734679, discloses a system in which the Hamming weights of randomly generated numbers is tested against a threshold value.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137